Attrition in Network Centric Warfare

John Erbetta
Defence Science and Technology Laboratory
Malvern Technology Centre, St Andrews Road
Malvern, Worcestershire WR14 3PS
UNITED KINGDOM
[44] 1684 771186

jherbetta@dstl.gov.uk

ABSTRACT

Network Centric Warfare (NCW) is concerned with exploiting information to maximise combat power. Integration of C2 systems is able to increase military effectiveness, whether in manoeuvre, engagement, logistics or protection. However this increases the potential length of the 'electronic' chain from 'sensor to shooter'. This paper has its focus on the issue that battle damage and force attrition (both equipment and human) occur in real conflict. The hypothesis is that at some point this may result in decreased force effectiveness rather than increased advantage. Information warfare means that positive attacks on systems themselves compound the problem. Emerging technologies applicable to NCW as a force multiplier need to be recognised as a counter to the impediments to progress that are recognised as inhibitors in the development of NCW. The impact of battle damage, attrition and cyber attack is addressed, as well as system security and the associated human factors of authority and responsibility. Options to minimise these vulnerabilities are postulated. The development of distributed systems and potential of using arbitration in decision making is viewed as one option to minimise the impact of performance on C2 effectiveness. The paper also recognises that whilst dominance (in its widest sense) is the ambition of symmetric warfare, this cannot be guaranteed whilst, in the asymmetric case, structures can be undermined by relatively unsophisticated attack. In particular the purpose is to underline the fact that implementations need to ensure that attrition results in 'graceful', rather than catastrophic, degradation. At the extreme end of the C2 performance spectrum the question must be asked how far can degraded C2 performance threaten force effectiveness. Assessment at this level is difficult and real answers are only likely to come from real life exercise that study the degree of reliance on C2 effectiveness during battle. The output will indicate the steps that need to be taken.

***Key Words**: Attrition, Network Centric Warfare.*

1.0 INTRODUCTION

1.1 Purpose

The purpose of this paper is to review the impact of attrition on Network Centric organisations faced with the attentions of a competent, knowledgeable adversary. It recognises that 'network centricity' is a growing feature of all organisations, the military not excepted. The extent and timeframes can be debated but already there is increasing integration of systems. It is considered that this trend will continue, possibly up to the point where all command and control systems are fully integrated with sensor and weapon systems. The burden of this paper is to underline that the entire system then becomes an entity which adversaries will target in what they regard as the most effective way.

Paper presented at the RTO SAS Symposium on "Analysis of the Military Effectiveness of Future C2 Concepts and Systems", held at NC3A, The Hague, The Netherlands, 23-25 April 2002, and published in RTO-MP-117.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
00 DEC 2003	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Attrition in Network Centric Warfare	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defence Science and Technology Laboratory Malvern Technology Centre, St Andrews Road Malvern, Worcestershire WR14 3PS UNITED KINGDOM**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001657., The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**16**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

The term adversary is used to cover the entire range of opponents from conventional forces, through 'conventional asymmetry' and terrorism to civil protest groups.

1.2 Network Centric Warfare

Network Centric Warfare [1] has been most clearly articulated in the open source material through the US Department of Defense publications. These papers have been used as the base for this discussion, whilst recognising that other nations have differing definitions and terms. Similar concepts are in development in non-military circles, indeed, NCW has been equated to e-business.

This paper is concerned with general principles in the integration of military systems (C2, sensors etc.). The US Department of Defense, through its C4ISR research programme has, in the unclassified literature, been most articulate in expressing the concept as Network Centric Warfare (NCW), defined as

"The tenets of NCW are:

- A robustly networked force improves information sharing
- Information sharing enhances the quality of information and shared situation awareness
- Shared situational awareness enables collaboration and self-synchronisation, and enhances sustainability and speed of command
- These, in turn, dramatically increase mission effectiveness

Within the concepts the impediments to progress are recognised and are summarised as including:

- Lack of secure, robust connectivity and interoperability
- Intolerance of disruptive innovation
- Lack of understanding of key aspects of human and organisational behaviours
- Lack of NCW-related technology investments"

(Source: NCW [1])

This paper is especially concerned with some of the latter issues. The basis is that we are steadily moving towards Network Centric concepts. Therefore we should clearly identify and assess the impact of specific attacks on the core of this new infrastructure. NCW can be analysed as a federation of systems. However a system that combines sensor to shooter capability is not simply a process but a battlespace platform in its own right. As such it will be a legitimate target for attack and its effectiveness will be measured not only by the way in which it performs (its fighting capability) but also on its defensive capability, its human resources and its damage control facilities.

In organisational terms, the impact of NCW is to move force structure towards a virtual organisation [2] effectively fragmenting traditional chains of command, and introducing clusters. Its impact on military organisation needs further work.

1.3 Purpose of Attack

The purpose of an attack is to deny key components within a weapon system to inhibit the OODA (Observe, Orient, Decide, Act) loop**.** Since a weapons system is a combination of one or more weapons, with all the related equipment, materials, services, personnel and means of delivery and deployment required for self-sufficiency, it follows that the NCW concept means that the planning and operational infrastructure must be included within that definition. Hence the NCW 'infrastructure' becomes as much a target as the sensors or weapon system.

It is this change, from Command and Control being a 'management' process to that of being part of an integrated weapon system, that means consideration of the impacts of specific attack should be considered in the evaluation of system of systems which have network centric attributes. Here one of the major issues is how to assign measures of merit. In particular a successful cyber attack is likely to be one that has not been anticipated. 'Sleeper' code (i.e. rogue software that is benign until triggered by time or an event) could have dramatic effects especially because the attack and its effects are separated by a time interval which could be months. Measures of merit do not exist in isolation and, for example, measuring the impact of C2 attrition needs to be mapped onto force effectiveness and related back to C2 effectiveness. If the wrong measure is used then it is conceivable that a major impact on C2 effectiveness could create a minor impact on force effectiveness whilst a 'minor' impact on C2 effectiveness would have a major impact on force effectiveness.

Robert Bunker [3] has written on the vulnerabilities of the Army After Next (AAN) to sophisticated cyber attack, one of the issues considered in this paper.

2.0 NATURE OF ATTRITION

2.1 Impact of Attrition

The word Attrition can be construed in a number of ways. Specifically any reduction in capability is included and in this is included battle damage, human casualties and cyber attack. The Shorter Oxford English Dictionary emphasises 'wearing or grinding down'. The burden of the paper is that evaluation must be made of the impact of this wearing away. For example, it should be possible to measure the impact of manpower attrition on C2 or force effectiveness and indeed create some relationship between the two. However if this is combined with equipment damage and cyber attack the impact on effectiveness at C2 and force levels is likely become more marked. The evaluation should not ignore such possibilities.

For the purposes of this paper 3 areas are considered at 3 levels:

- the levels are personnel, military sensor/command/weapon systems and infrastructure.
- the attacks will be against manpower, equipment and cyber targets.

Target \ area	Personnel	Systems	Infrastructure
Manpower	Primary Impact	Secondary Impact	Secondary Impact
Equipment		Primary Impact	Primary or Secondary Impact
Cyber	Secondary Impact	Primary Impact	Secondary Impact

A successful attack aimed at personnel will have a primary impact on force structure but is likely to have a secondary impact on systems and infrastructure, as support to these areas will depleted.

Successful attack on equipment will have not have a direct impact on personnel but may have an impact on infrastructure.

A successful cyber attack will primarily impact on systems but may well have a secondary impact on infrastructure and human (e.g. misinformation).

2.2 Manpower Attrition

Manpower attrition can be both temporary and permanent. The prospect of the use of chemical or biological weapons has potentially broader impact on network centric operations than in conventional

operations. In modelling (or other form of assessment) manpower attrition in NCW it is important that all impacts are considered. Manpower has an impact on all four lower levels of Measures of Merit (see [4] Figure 5.1). The reason for this is that even the lowest level (Dimensional Parameters) such as the network 'wiring' is dependent on people.

2.3 Equipment Damage

Damage can be caused though direct or indirect attack (and indeed accidental damage should not be excluded). In the first place destruction of the nodes (or of essential supporting facilities e.g. electricity supplies) must be considered. This should be assessed on a physical basis (i.e. what components are situated in a particular area or building). Theoretical assessments may consider networks as separate entities but frequently they are co-sited with other elements from other networks.

The conventional measures such as quality of service and mean time to repair can be dramatically changed if there is significant, co-located damage (and it should be recognised, in evaluation, that network and human casualties may occur simultaneously). This, in network centric operations, could have significant impact on force effectiveness.

Networks are becoming increasingly sophisticated. The move away from conventional 'wirebased' systems to wireless and complex photonic systems means that systems performance in extreme circumstances becomes uncertain. Systems being installed and being planned have significant, in built, redundancy. However their performance under stress is complex. In significant incidents reduction in capacity results in an increase of traffic. Again the determination of appropriate measures of merit needs careful consideration.

3.0 THE ISSUE

3.1 NCW Provides Competitive Advantage

The objective of warfare is to achieve dominance. Reliable Command and Control systems, used in the decision making process, speeds decision making. As more systems are integrated the improvement in the speed and accuracy of the command process increases. In the competitive environment that is today's battlespace success in this area equates to competitive advantage. In the first stage this advantage is in information dominance but as this develops to encompass more and more systems (the vision that is NCW) this translates into battlespace dominance, NCW providing the way of optimising resources to achieve this purpose.

This vision is reflected in the linkages from measuring performance through to measuring force effectiveness and even policy effectiveness. Therefore it is important that measures should be introduced, at each stage, to ensure measurement (and validation) of the objectives.

3.2 Attrition

This paper is focused on the implications of the decision support process components suffering attrition. The questions that arise are:

- How does the system of systems perform when it suffers from equipment damage?
- Can cyber attack actually provide misinformation?
- Is there an issue of system of systems stability?

These, of course, are the technical issues addressed to the lower Measures of Merit levels. More importantly is consideration of the how this degradation impacts on warfighting capability. Associated is the impact of manpower loss in the context of NCW. This extends beyond 'front line' personnel through various levels to those who are responsible for the maintenance of equipment. In many cases the number of people who actually understand the full complexity of an individual system is limited. When integrated into a system of systems this becomes even more fraught! Additionally, in the days of multinational defence corporations who may be supplying more than one party in a conflict, objective analysis becomes even more complex!

Cyber attack takes many forms. Indeed in most cases the successful attacks are those which exploit an unknown weakness. It is therefore conceivable that an attack could change data or add new data. Ideally the system would be able to distinguish such data but thought needs to be given to the assessment of the impact of a successful attack.

The final question is the question of stability - is the transition from full effectiveness abrupt and if so, under what conditions? This is discussed below.

3.3 Styles of Failure

The performance of complex system under stress is complex and the nature of failure of system of systems is incomplete. Obviously there will be performance limitations of any systems. Usually there is sufficient redundancy for high loading and limited component failures to have minimal impact. A network centric system of systems potentially will substantially outperform conventional systems in most circumstances – see Fig 1. However at a certain point the system will start to overload and it is considered that catastrophic failure might well occur. This will be as a result of one or more of the following:

- Data/Information overload
- Damage to components
- Cyber attack
- Manpower loss

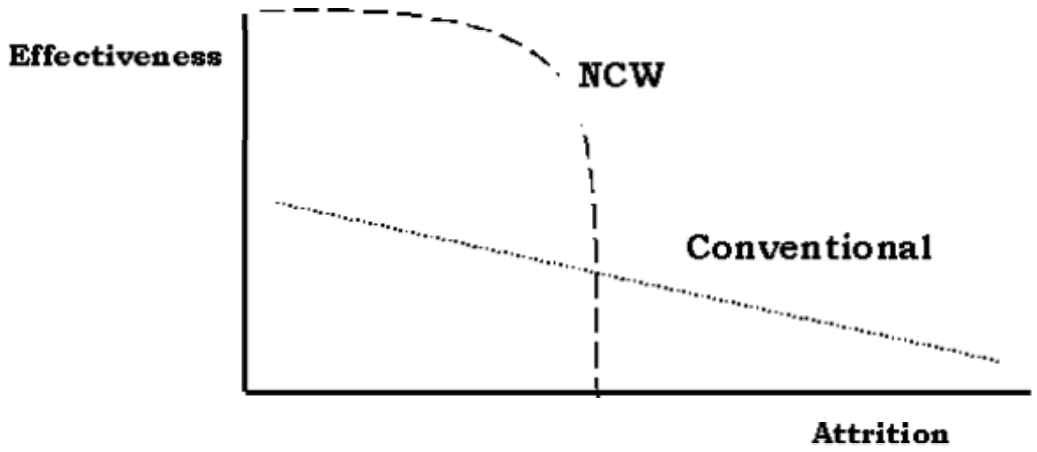


Figure 1: Relationship between C2 Effectiveness and Attrition.

Whether or not this hypothesis is valid depends on a number of factors, not least on where system boundaries are drawn! However what is clear is that there is a need to further investigate this area to evaluate the implications for force effectiveness.

4.0 DEVELOPMENT OF NETWORK CENTRIC CONCEPTS

4.1 Recognised Inhibitors

It is recognised that there are a number of technology areas that need to be developed before NCW becomes fully viable. Similarly the understanding of related human and organisational behaviours in virtual organisations, especially related to command structures, is still limited. Evaluation of the overall system must take account of these factors.

4.2 Emerging Technologies

Network Centric Warfare is an emerging concept that is only likely to become viable in the next two decades. The incorporation of emerging technologies is crucial for success. Optimum use of resource will only be obtained if the criteria applied to evaluation are also used for the assessment of the emerging technology.

4.3 Authority and Responsibility

Currently machines largely operate in ways which have been predetermined. For example, a machine would have a list of people who are permitted to see certain information and would rigorously enforce this requirement. This formality has certain advantages in normal operation. However it is possible to conceive of (but not predict) instances when this rigorous separation may need to be overruled. In human based systems it is easy to see how this would be achieved, through the exercise of authority and with it a responsibility that in the circumstances a breach of the rules was for a ‘higher good’.

In developing network centric concepts it will be seen that the issue of authority and responsibility needs to be adequately covered. The extreme need for this is likely to occur if an effective cyber attack were launched. Information from the system of systems may lead to a conclusion that is contrary to the (human) logic of the commander on the ground or in an HQ. A human judgement must be capable of being inserted into the system (with all the current ‘checks and balances’).

4.4 Planning

The radical nature of NCW means that long term planning should recognise the emergence of this powerful but innovative approach. It is likely that approaches based on incremental, budget-based, risk avoidance and historical extension will be found wanting. Technology based approaches offer significant risk as this paper has sought to outline. Scenario-based and capability-based planning approaches may well be most valuable, provided that sufficient consideration is given to the issues of attrition and that due recognition is given to the nature of ‘system of systems’.

5.0 MINIMISING VULNERABILITIES

5.1 Technology Watch

Technology never stands still! The vulnerabilities and options for attack of NCW will constantly develop. The application of technology watching approaches should enable those developing systems not only to utilise new approaches to optimise their own systems but should also make them aware of new and emerging threats to their own systems from adversaries.

5.2 Management

Vulnerabilities can be minimised by the used of appropriate management techniques. However to be successful the issues that need management must be clearly delineated. The use of technology must be

managed with regard to warfighting needs, not allowing the technology needs to become dominant. This has significant organisational implications, developing an appropriate paradigm that takes account of stakeholder aspirations, whilst suitably managing expectations!

5.3 Technological Solutions

Various technologies are maturing that potentially could provide at least partial solutions. These are given as examples of the fact that technology is moving forward. However, assessment of network centric solutions must recognise that rapid technological developments will impact on the effectiveness of system of systems.

The use of arbitration (taking a number of independently derived solutions and using arbitration to identify errors) is emerging for use in secure systems. This has its roots in avionic systems which, with their need for providing timecritical and accurate information, use multiple systems to produce a number of results with 'majority voting' identifying any systems errors.

A significant number of programmes in both civil and defence sectors are looking a range of approaches using distributed systems that can produce secure, reliable and resilient results. These provide greater resistance against failure but their value has to be measured not only by their reliance but also their performance in failure. Again the final measure is the impact on force effectiveness.

6.0 THE WAY AHEAD

6.1 Research

The full concept of NCW is at this stage still in its infancy. It is anticipated that over the next 20 years there will be significant strides in realising effective integrated system of systems. What is almost certain is that what will the solutions realised will have features that we cannot imagine at this time. Research will continue to play a key part in the development of network centric solutions.

6.2 Implementation

Effective learning comes not only out of the laboratory but also from the lessons learnt from current (and past) systems. Over-ambitious planning and procurement have often led to non-optimal systems and there is a need to balance desires with that which can be achieved in a timely and cost effective manner. The analysis of alternatives [5] is complex especially when the issue of cost is encountered. It is important that the measures of merit used are independently assessed otherwise there can be unintentional bias.

6.3 Management

Known problems can be managed. This paper has underlined the fact that, like all new technologies, NCW brings benefits but also produces fresh issues. The issues should not be allowed to obscure the benefits and the solution lies in the way in which systems are managed. In particular NCW emphasises the need to view the support infrastructure (and its management) as an integral part of the whole equipment capability. There should be seamless management from sensor to shooter including C4I.

6.4 Doctrine

The impact of new technologies and structures (that are implicit in NCW) will result in new doctrine being developed. This must ensure that the impact of attrition will be minimised. This is a complex matter and will impact on evaluation.

6.5 Assessment

Assessment of the impact of attrition must be carefully undertaken. The modelling of systems must be capable of reflecting manpower and equipment attrition as well as the impact of cyber attack (perhaps the most difficult to model!). However assessment is not the end and, with the evaluation of alternatives [4], enable systems matching needs (and providing optimal cost benefits) may be procured.

7.0 CONCLUSIONS

'Full Spectrum Dominance' [5] will, to a greater or lesser extent, embrace NCW concepts. Evaluation of systems of systems requires consideration of the impact of attrition. This consideration extends well beyond availability and quality of service issues through the impact of battle damage, manpower attrition and cyber attack to force effectiveness. It moves from dimensional parameters to measures of force effectiveness.

The NATO Code of Best Practice [4] provides a valuable framework. However the evaluation should not simply be a passive analysis producing negative views but assist in engaging a positive review of the options that can be taken to overcome these issues. Above all it enables the effects of attrition in complex systems with high degrees of interdependence to be evaluated in a structured manner.

8.0 REFERENCES

[1] Alberts, D.S., Garstka, J.J. and Stein, F.P., *Network Centric Warfare*, US Department of Defence C4ISR Cooperative Research Program – February 2000.

[2] Hughes, J.A. et al, *Some 'Real' Problems of 'Virtual' Organisations,* Lancaster University 1998.

[3] Bunker, Robert J., *Five-dimensional (Cyber) Warfighting: Can the Army After Next be Defeated through Complex Concepts and Technologies?,* U.S. Army War College – August, 1998.

[4] *Code of Best Practice for Command and Control* – NATO – Revised Edition 2002.

[5] AoA Handbook, *A Guide for Performing Analysis of Alternatives,* Office of Aerospace Studies – June 2000.

[6] *Concept for Future Joint Operations* – US Department of Defense – May 1997.

9.0 ACKNOWLEDGEMENT

The author is grateful to colleagues in Dstl for support during the writing of this paper. The paper has been written from open source material and does not necessarily reflect the views of Dstl or any other official body.

AUTHOR BIOGRAPHY

John Erbetta is with the UK Defence Science and Technology Laboratory. He read Engineering at University and then undertook postgraduate studies in systems engineering and later gained an MBA. With extensive experience in both public and private sectors, he is the author of a number of papers.

Attrition in Network Centric Warfare

John Erbetta

Defence Science and Technology Laboratory

Malvern Technology Centre WR14 3PS UK

This presentation represents the personal views of the author and should not be taken to represent the view of either Dstl or any other official body.

Introduction to Network Centric Warfare

- **Outline description**
- **System of Systems**
- **Long ‘sensor to shooter’ chain.**
- **Impact of automation on C4I**
- **BUT major change is that C4I systems are becoming ‘weapons’ and therefore susceptible to attack**

Nature of Attrition in real conflict

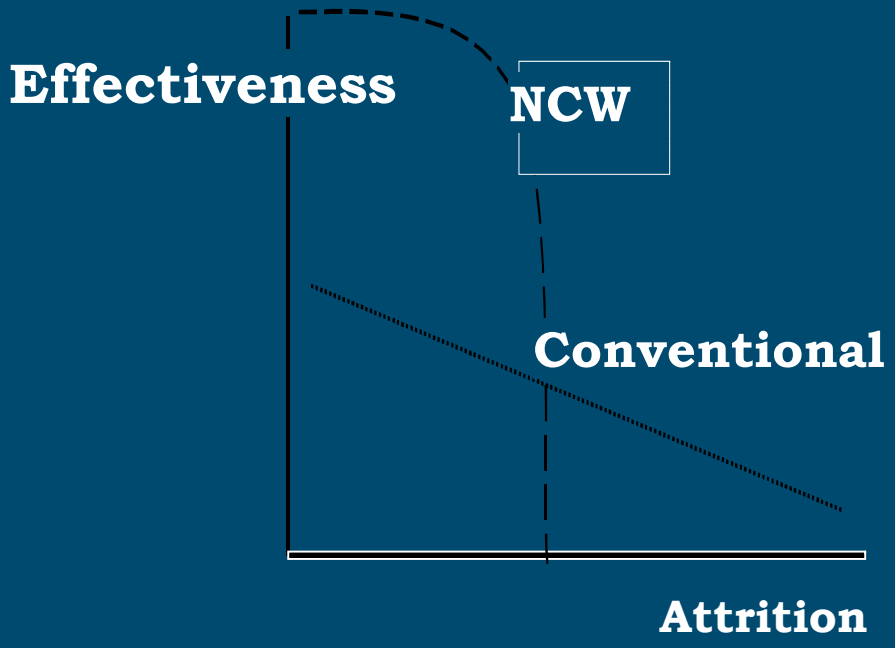
- **Equipment (including communications) battle damage**
- **Human casualties**
- **Cyber warfare**

The Issue

- **Reliable ‘automated’ C4I provides increased advantage**
- **Unreliability of such systems results in, at:**
  - **Best - decreased effectiveness**
  - **Worst - total confusion**

Failure in Network Centric systems

- Under moderate ‘loads’
  - High reliability
  - No impact with moderate loads
- BUT!! When it happens
  - Rapid decline
    - Data/info overload
    - Damage
    - Cyber Attack
    - Manpower



Development of Network Centric Warfare

- **Recognised inhibitors**
- **Emerging technologies**
- **Authority and responsibility.**
- **Analysis of impact of:**
  - **Battle damage**
  - **Attrition**
  - **Cyber attack**

Minimising vulnerabilities

- **Technology watch**
- **Management options**
- **Distributed systems**

Assessment Issues

- **Defining attrition types**
  - **‘Normal’ Damage**
  - **Human Impact**
  - **Modelling cyber attacks**
- **Analysis of Alternatives**
- **Measures of Merit**
- **Force Effectiveness**